**MotorHead Distributors Audit Report**

Table of Contents

1. [Overview](#Overview)
2. [Network Architecture](#Network)
3. [Data Handling](#Data)
4. [Risk and Policies](#Policies)
5. [Executive Summary](#Summary)

**Ov****erview**

The audit looks at three main components: the network architecture, data handling, and risk and policies. These three topics are explored with the intention of improving both security and efficiency within Motorhead Distributors. Serious errors have been found that need to be corrected if Motorhead is to remain competitive and reliable.

**Network Architecture**

The network diagram provided reveals a shamefully simplistic network design for an organization of Motorhead Distributors’ size. There are virtually no layers of security. In fact, beyond access control, flimsy firewalls are the sole protectors of the entire network. There are no redundancies in the event of a devices failure. The most prominent weakness of the system is a singular internet facing router and firewall. That becomes a major bottleneck for inbound and outbound traffic and, thus, a prime target for attack. Also, what happens when the outmost router crashes?

The saving grace of this network is its ability to handle copious amounts of internal and end user traffic. An issue appears here as well, however, in the form of wireless access points. All the wireless access points connect directly to the network without any protection, meaning anyone onsite has unrestricted access. One point even goes directly to a major switch. Such a direct connection is potentially a serious problem. There should be a greater separation of devices to limit this connectivity, especially for these more vulnerable points.

There is a definitive lack of layers in this network. Lacking these layers is the leading cause of issues, swiftly followed by the absence of any kind of redundancy. Our suggestion would be to restructure the architecture to incorporate layered security as well as redundant systems to fail over to in the event a device goes down. Most important will be the addition of a DMZ, or De-Militarized Zone.

DMZ

A DMZ would greatly benefit the company by helping to make the network structure more secure from outside infiltration. Effectively, a DMZ separates key systems requiring the most protection and those systems that customers will need to access from off site. This creates a nearly separate environment void of any critical systems, which protects the network as a whole from attack. Individual devices and systems are also made more difficult to penetrate. In addition to the protection, it separates internal end user traffic from external traffic alleviating any potential congestion as well as the impact of device failure.

**Data Handling**

Due to Motorhead Distributors only processing transactional and customer data there are almost no laws that apply strictly to the handling of your data or the securing of said data. While there are certain practices that help to ensure data confidentiality, integrity, and availability, no laws currently regulate them. We believe the previously mentioned layered restructuring will be a sufficient shield from potential threats. Given the minimal data loss and interruptions in the past, there is only one other suggestion we have, and that is encryption.

The data that needs encrypting is the most important data on hand, customer information. They will want to know that their personal, private information is safe and being treated as a high priority. Not only do we want customers to feel safe using our services, but that information will be of the most worth to an infiltrator.

This is not to say that customer information is the only data that should be encrypted, just that it needs to be an extremely high priority. Other systems could benefit from encryption as well, such as product logs and communications. Both customer information and communications data, such as emails, will need to be encrypted at rest as well as in transit. Any other data can be maintained at rest.

Policies and procedures regarding encryption should be treated with the same esteem and regard financial transactions and policies are given. They are nearly as important in that they are the life blood of any business.

Improvements to the security will need to be the kind of culture shift that only works from top management down to everyone else, all the way to the janitorial staff.

**Risk and Policies**

Motorhead Distributor’s current attitude toward information security presents challenges. There is a “laid back” stance in regard to security. That stance is breeding a corporate culture that will end up disregarding it completely on the most important level, end users. A serious emphasis on staying safe must come from the top. A particularly important component is an emphasis on proactive and preventative measures as opposed to the generally reactive steps the policies outlined prior to this review.

Motorhead should be more strict on its adherence to risk analysis and reassessment. This goes back to the attitude issues previously mentioned. As of now any risk assessments are working as a “feel good” tool, not something up to date and useful. Knowing what could go wrong and how bad it could be is imperative to staying prepared for any indent, big or small. Constant self-assessment is the only way to stay ready for the inevitable.

What needs to happen is more idealistic than paper oriented. There will need to be a culture shift away from reacting and toward proactive mitigation. While Motorhead has been comfortable with their IT systems in the past, the company as a whole will need to recognize that it is generally better to pay out up front rather than later. Those upfront costs come in the form of updating and replacing both software and hardware. Done properly the downtime is minimal and customers don’t experience any issues.

Something worth noting here is customer’s credit card safety. There is no risk to Motorhead Distributors of exposure when customers use their credit card. All risk associated with credit card transactions falls on our third party processor regardless of our downtime or system failure. Motorhead’s processing vendor is more than certified and has served well in the past. This risk is minimal to nonexistent for Motorhead Distributors.

Other risks documentation has not been revised for Motorhead Distributors. No issue specific or system specific policies have been defined as per this audit. Enterprise and organization wide policies have been revised, however. This includes a disaster recovery plan and security response plans. These documents won’t help do reduce risk, but assist in handling any given event. Major risks should be looked at more closely and documented individually.

Contingency Plan

Redundant systems and backups need to the first line of defense. Those will be the quickest, most efficient use of time and resources to get systems back up and running. Having something to fail over to in the meantime is the next highest priority. Assuming both fail, there will need to be staff constantly on hand that can rebuild any system that might fail. This could mean cross-training employees.

The best option may be to outsource all backups or, at least, store them off site. There will need to be a great deal of data retained due to the nature of Motorhead’s business. Customer information is chief among them swiftly followed by the financial information tied to those customers. Much of that data, in particular data on customers no longer using services, can be archived and moved off of the main servers to an offsite location as well. In this way efficiency is maintained, and system clutter is reduced.

**Executiv****e Summary**

The audit reviewed three main components: the network architecture, data handling, and risk and policies. These three topics were explored with the intention of improving both security and efficiency within Motorhead Distributors. Serious errors have been found that need to be corrected if Motorhead is to remain competitive and reliable. The major fixes are: a corporate culture change toward proactive security, a rework of the network architecture, implementation of redundant systems, and revision of current policies. In addition to these items, a regular review of policy should be implemented as well as annual risk assessments. Once the changes are made, Motorhead will me markedly more secure and prepared for any incident that might occur.